Review and Analysis

Introduction

The FDIC's compliance examination process assesses how well a financial institution manages compliance with federal consumer protection laws and regulations. The review and analysis phase of the compliance examination starts with a top-down, comprehensive evaluation of the compliance management system (CMS) used by the financial institution to identify, monitor, and manage its compliance responsibilities and risks. The procedures outlined below guide the examiner through an assessment of an institution's CMS, and assist the examiner in identifying specific areas of weakness for further analysis. Many procedures listed in this section can be performed at the field office or other location prior to the on-site portion of the examination, if materials are available.

Off-Site Review and Analysis

The Examiner-in-Charge (EIC) reviews and analyzes the material gathered from FDIC, third parties, and the institution in response to the Compliance Request Letter in order to develop the risk profile and scope memorandum and plan the on-site portion of the examination. This review and analysis should be broad enough to obtain an understanding of the organizational structure of the institution, its related activities, and compliance risks associated with each of its activities. The review should be used to preliminarily determine whether the institution's management and Board of Directors identify, understand, and adequately control the elements of risks facing the financial institution. In general, management and Directors are expected to have a clearly defined system of risk management controls governing the institution's compliance operations, including those activities conducted by affiliates and third party vendors. During this review the EIC should consider what types of questions should be asked while on-site to test whether the bank's written policies and procedures accurately reflect actual operations.

Risk Profile and Scope Memorandum

The goal of a risk-focused, process-oriented examination is to direct resources toward areas with higher degrees of risk. To accomplish this goal, the examiner must assess the financial institution's CMS as it applies to key operational areas, and evaluate the risk of non-compliance with applicable laws and regulations. The result of this assessment is the Risk Profile, a matrix and narrative that summarizes the perceived risks, and provide the basis for preparing the Scope Memorandum. The Scope Memorandum describes the focus of the examination, including issues to be investigated and regulatory areas to be targeted during the examination.

A Risk Profile and Scope Memorandum template should be downloaded from SOURCE at the beginning of the examination process. SOURCE will automatically populate it with relevant information from other FDIC databases. After conducting the off-site review and analysis, the examiner should document the preliminary risk assessment and expected examination scope in the Risk Profile and Scope Memorandum, and obtain and document appropriate approval. During the examination the EIC should obtain approval for any material changes to the scope of the examination, in accordance with regional or field office requirements.

At the conclusion of the examination the EIC must review the preliminary Risk Profile and Scope Memorandum developed at the beginning of the examination and edit it as needed to reflect the post-examination risk assessment of the institution, and the actual scope of the examination. The final Risk Profile and Scope Memorandum should be posted to SOURCE, making it available to all staff and management during the exam review and for future internal use, especially for the start of the subsequent examination.

Additional information about crafting the Risk Profile and Scope Memorandum is provided in the following sections.

Developing a Risk Profile

In order to properly assess a financial institution's risk, the EIC or designee reviews the following primary areas:

Compliance Management System:

- Management and Director Oversight
- Compliance Program
  - Policies and Procedures
  - Training
  - Monitoring Procedures
  - Complaint Response
- Audit Procedures

Operational Areas:

- Lending
- Deposits
- Insurance Sales
- Investment Sales
- Other Products or Issues

The resulting risk profile compares the strength of the CMS to the risks attendant to particular operational areas.

While reviewing a bank's operations, the examiner should consider the impact of the following types of risk:

Performance Risk:

- Current & Past Enforcement Actions
- Reimbursement History
- History of Compliance with Fair Lending laws

- Current and Prior Regulator Ratings
- Audit Findings

Regulation Risk:

- Applicable Regulations
- New Regulations
- Changes to Regulations
- Recent Case Law

Product Risk:

- Major Product Line
- New Products/Services
- Growth in Operations
- Complexity of Operations
- Third-party Affiliations

Performance Risk: The financial institution's past compliance performance is an important consideration when developing its risk profile. Historic effectiveness of the compliance management system, including the results of previous examinations and management's record of taking corrective measures, will impact its risk profile and ultimately, the scope of the examination. The most recent compliance history should be given the most weight. The EIC will be able to locate performance risk information in various areas, including the FDIC's correspondence and enforcement records for the subject institution. The most recent Risk Management report and workpapers may contain additional information on the bank's performance risk (e.g. comments regarding institution management).

Regulation Risk: Regulation risk measures the possible consequences to the bank and its customers of noncompliance with specific regulatory provisions. Regulation risk recognizes that the impact of noncompliance differs depending on the consumer law or regulation. For the public, it is the measurement of relative adverse financial impact or other harm that noncompliance may produce. For the bank, regulation risk is the measurement of legal, reputation, and financial harm that noncompliance may produce. For example, the financial harm both to the bank and to consumers associated with violations of the Truth in Lending Act (Regulation Z) requiring reimbursements far exceeds the consequences of an isolated undocumented check hold. The level of regulation risk is affected by such factors as:

- Potential financial and/or reputation harm to consumers;
- Potential legal, reputation, and financial harm to a bank;
- New laws, regulations or amendments thereof; and
- The amount of transaction activity subject to a specific regulation.

Product Risk: The institution's products and services impact the bank's risk depending upon the financial institution's size, market share and portfolio concentration. The complexity of products offered and the associated likelihood of error should be considered. Third party affiliations, particularly for product delivery, present heightened risk. Finally, the institution's strategic plan for growth and for the introduction of new products and services should also be taken into account.

Taking into consideration the conclusions drawn in each of the preceding components, and any other pertinent information, the examiner should develop a risk profile of the institution by assigning and adequately supporting a category of Low, Moderate, or High compliance risk for each CMS element and operational area. An institution with a Low Risk Profile in a particular area will effectively manage compliance risks. The institution's Board and management actively participate in managing the CMS, the CMS is considered strong, and historic examinations support this assessment. Spot checks of transactions may be appropriate to verify continued strength. An institution with a Moderate Risk Profile is generally effective, but specific weaknesses are identified or suspected. Some particularized transaction testing should be planned. An institution with a High Risk Profile is ineffective in identifying, monitoring, or managing compliance risks in particular operational areas. Significant risk is readily apparent and may be supported by prior examination findings. Institutions in this category will require more extensive transaction testing in light of the risks of non-compliance. (Specific issues to be investigated and areas to be targeted with transaction testing should be addressed in the Scope Memorandum, which is discussed in the next Section.)

It is important to remember that one element of a financial institution's compliance efforts may influence another area. Be aware of relationships and their mutual impact. For example, if the initial review of bank practices identifies a lack of audit of loan denials, the examiner should look to see whether monitoring procedures are in place to mitigate the impact of the lack of audit procedures. The existence of monitoring procedures may lead the examiner to determine that the absence of an audit does not raise the institution's risk profile. Conversely, if the initial review of bank policies and procedures identifies well-organized written guidelines for deposit compliance management, the examiner should also consider the bank's record of oversight in this area. If deposit compliance has historically suffered from poor management oversight, then the existence of written procedures should be given less weight when determining the risk profile.

The following matrix should be completed as an illustration of the bank's overall Risk Profile. Each column/row intersection should be labeled as presenting a (L)ow, (M)oderate, or (H)igh level of compliance risk for the institution. The narrative accompanying the matrix should summarize the perceived risks with sufficient information to support the risk ratings, including particular performance, regulation or product risks.